Assessment of Public Comments for New Part 500 to 23 NYCRR

The New York State Department of Financial Services (the "Department" or "DFS") received over 150 comments on proposed rule 23 NYCRR 500 from individuals and entities, including a variety of regulated entities and trade associations, as well as from third party service providers, including cybersecurity service providers, and others. These comments are summarized as follows.

Many commentators commended the Department for its efforts in addressing cybersecurity. Some commentators suggested that DFS expand or heighten the proposed regulation's requirements by, for example, setting a time limit within which Covered Entities would be required to have identified a breach; requiring Covered Entities to perform more testing of their systems and to retain outside consultants for testing; and mandating additional cybersecurity measures. DFS believes that the proposed regulation effectively addresses the required elements of a cybersecurity program at this time, along with DFS's overall supervisory authority.

A number of commentators supported the proposal's goal to set minimum standards for cybersecurity practices, so that cybersecurity programs match the relevant risks and keep pace with technological advances. Commentators asserted that provisions in the regulation should be made more flexible and risk-based. DFS has clarified in the revised regulation that certain requirements are linked to the results of the Covered Entity's Risk Assessment, consistently with the proposal's original stated intent. To be clear, the Department believes that each Covered Entity should model its cybersecurity program on the Covered Entity's cybersecurity risks, but the Risk Assessment is not intended to permit a cost-benefit analysis of acceptable losses where an institution is faced with cybersecurity risks.

Commentators requested clarification, tailoring and/or narrowing of certain definitions, including the following:

Cybersecurity Event: Some commentators stated that this definition, and particularly its use of words like "unsuccessful" and "attempt," was overbroad and resulted in overbroad requirements. DFS has not revised this

definition because it is important for a comprehensive cybersecurity program to address attempts even where unsuccessful. However, the Department has revised several of the provisions of specific concern by requiring that certain provisions be based on the Risk Assessment and by including materiality qualifiers, such as in the Notices to Superintendent section.

Information System: Some commentators stated that this definition is overbroad and resulted in overbroad requirements. The Department has not revised this definition because the Department believes its scope is appropriate in the context of the revised proposed regulation.

Nonpublic Information: Commentators variously asserted that this definition is overbroad or unclear, or argued that it should more closely track the language of other standards in order to, for example, reduce the need for entities to classify data in multiple ways when attempting to meet the requirements of different regulations or laws. The Department has made several revisions to this definition in response to these comments.

Publicly Available Information: Some commentators asserted that this definition is too narrow and should encompass more information, or should otherwise be revised. The Department has not revised this definition because the Department believes it is appropriate in the context of the revised proposed regulation.

Some commentators questioned the use of the term Chief Information Security Officer ("CISO") – specifically, that the regulation might require hiring or appointing an individual whose exclusive job would be to serve as a CISO under that specific title. In response, DFS has revised section 500.04 to clarify that each Covered Entity shall designate a qualified individual to perform the functions of a CISO, but that DFS is not requiring a specific title, or an individual exclusively dedicated to CISO activity.

Commentators asserted that a variety of other specific provisions were overly prescriptive and/or insufficiently tied to the results of the Risk Assessment. In many cases, commentators suggested specific alternative language to address such issues. The Department has revised the Risk Assessment section (500.09) and other sections to clarify and/or make more explicit the Department's original intent to have risk-based

requirements tied to the Covered Entity's Risk Assessment as provided in the overall regulation and the Department's supervisory authority. Risk Assessment is now a defined term. In addition, revisions have been made to the following sections: Cybersecurity Program (500.02), Cybersecurity Policy (500.03), Penetration Testing and Vulnerability Assessments (500.05), Access Privileges (500.07), Multi-Factor Authentication (500.12), and Encryption of Nonpublic Information (500.15).

Some commentators stated that requirements in the Cybersecurity Personnel and Intelligence section (500.10) and the Training and Monitoring section (500.14) should be more risk-based. In response, the Department revised these sections to, among other things, more specifically tailor certain requirements.

Some commentators asserted that the requirements of the Audit Trail section (500.06) were overly broad, leading to the capture and retention of too much information. In addition, some commentators claimed that the six-year retention period was too long. In response, the Department has made certain revisions to section 500.06, including amending section 500.06(a) to be explicitly based on the Risk Assessment and decreasing the retention period in section 500.06(b) to five years.

A number of commentators expressed concerns that the Limitations on Data Retention section (500.13) does not sufficiently take into account certain legitimate business reasons for which data might be retained. The Department has revised section 500.13 to explicitly take into account circumstances where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Commentators also stated that the requirements in section 500.11 regarding third parties doing business with a Covered Entity were too prescriptive, especially the preferred contract provisions. Commentators also expressed concerns that many Covered Entities would have difficulty complying because they would not have sufficient leverage over third parties to effect some of the proposal's requirements. In addition, commentators expressed concern that the required annual assessment for all third party service providers would be burdensome, given the large number of third party service providers used by some Covered Entities. The Department has

amended this section so that its requirements are more explicitly based on the Covered Entity's Risk Assessment. In addition, DFS has eliminated a provision in section 500.11(b) that may have unintentionally suggested that Covered Entities are required to audit the systems of all third party service providers. Also, in response to comments seeking greater clarity in regard to the requirements of this section, the Department has added a defined term, "Third Party Service Provider(s)."

Commentators claimed that the proposal includes overly broad reporting requirements that would result in many reports that are of little cybersecurity value. Additionally, commentators claimed that a 72-hour reporting timeframe is too short. Some commentators noted, for example, that in the first few days of a Cybersecurity Event, the entity is still gathering information on what happened. Also, commentators expressed concern about the confidentiality of notices provided to the Department. Based on its experience, the Department believes that the 72-hour reporting timeframe is essential to protect the markets while the Department does not intend for the reporting to include unnecessary information. Accordingly, the Department has revised section 500.17 to state that notice is required within 72 hours of a determination that a Cybersecurity Event as follows has occurred: (1) Cybersecurity Events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, and (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. In addition, DFS has added a confidentiality section to the proposed regulation.

Some commentators asserted that the annual certification requirement of section 500.17(b) should be eliminated. They argued, for example, that the annual certification requirement is unnecessary, or that compliance with the requirement would be costly and divert resources from other uses. Other commentators sought revisions in the annual certification requirement and/or certification form. The Department has determined that the annual certification is an important part of the regulation and the Department's oversight of the financial market. The Department does not believe that the requirement creates unnecessary burdens; to the contrary, the Department

believes the process is essential to good corporate governance. Accordingly, the Department has retained the annual certification requirement and the certification form included as Appendix A. In addition, the Department has determined that the content of the certification form and certification requirement are appropriate in the context of the revised proposed regulation.

Certain entities requested exemptions, but the Department determined not to alter the definition of Covered Entities, which in the Department's view provides adequate guidance as to which entities are covered. Some businesses, including small businesses, expressed concerns regarding cost and burden. The Department has included in the revised proposal several exemptions based on the risk that particular entities or circumstances present:

- The Department has included a limited exemption for a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not control, generate, receive or possess Nonpublic Information.
- The Department has included an exemption for an employee, agent, representative, designee or Affiliate of a Covered Entity, who is itself a Covered Entity, to the extent that the employee, agent, representative, designee or Affiliate is covered by the cybersecurity program of the Covered Entity.
- The Department has amended the limited exemption in section 500.19(a) by adding Covered Entities with fewer than 10 employees including independent contractors, deleting Covered Entities with fewer than 1000 customers in each of the last three calendar years, and changing "and" to "or" in two locations.

The Department has also added a notice of exemption filing requirement for entities claiming an exemption.

Multiple commentators expressed concern about the implementation timeframes. The Department has added to the Transitional Periods section of the revised proposal (500.22) a number of additional transitional periods. These additional transitional periods are designed to provide outside deadlines for compliance with

specific requirements, while urging Covered Entities to comply as soon as possible in order to protect customer data.

Some commentators asserted that the proposed regulation should harmonize more closely with other standards, including state, federal and international standards, both existing and proposed. The Department has been continually mindful of other standards and approaches and believes that the revised regulation is appropriately consistent with the goal of setting minimum standards.

Several commentators stated that all minimum standards should be eliminated and the Department should either (1) release guidance rather than promulgate a regulation or (2) wait for the federal government to promulgate regulations. The Department has not accepted any such suggestions, as the Department continues to believe that it should promptly promulgate a cybersecurity regulation as time is of the essence regarding cybersecurity protections. For similar reasons, no revisions have been made by the Department in response to comments that Covered Entities should be allowed to develop their own risk based controls, or otherwise follow other standards, in lieu of meeting the regulation's requirements.